CHIPS: Does Navy ERP replace legacy applications?

Keen: Yes. Navy ERP will replace a significant number of legacy applications. As we work with commands, we talk with them specifically about the applications that will be replaced as they learn the essentials about the functionality that the solution delivers. The Navy's Functional Area Managers (FAMs) are tasked with reviewing and determining which systems are to be replaced, and so our legacy system sunset plan is part of their plan. Right now, we're at more than 300 legacy systems that we anticipate replacing with Navy ERP.

CHIPS: Replacing 300 legacy systems will be a major transformation for the Navy.

Rosenthal: First, our Navy, indeed our whole military, is being asked to transform the way they accomplish their mission. Our troops are using technology in different ways than ever before, are organizing in new and different ways, and are being required to be more efficient and more effective at the same time. Those warfighters are the people the business side of the Navy supports.

On the business side, and I also call it the support side, we have an obligation to be as technologically advanced as we ask the warfighters to be, to organize to be agile in new and innovative ways to better support them, and to be as effective and efficient. Support for a transformed warfighting force must be provided by business systems that are also transformed. Navy ERP propels that transformation in Navy business affairs.

Secondly, many people and organizations use the word transformation. To put transformation into the proper perspective, I would share with you a quote I saw from Secretary of Defense Rumsfeld about business transformation.

'It is not, in the end, about business practices, nor is it the goal to improve figures on the bottom line. It's about the security of the United States of America. And let there be no mistake, it is a matter of life and death. Our job is defending America, and if we cannot change the way we do business, then we cannot do our job well, and we must.' That really sums it up.

Keen: I have been working in Navy IT, Navy information technology, for 28 years as a civil servant. This is the most important business transformation initiative based on IT that I have ever been part of. It's really an exciting program that will make a difference to our Navy and how we support the warfighter.

Rosenthal: Both Susan and I volunteered to do this because of the opportunity. The Navy ERP Program is probably the biggest challenge that either of us has undertaken. We consider it a privilege and an honor to serve the Navy in the delivery of this solution.

For more information about Navy ERP go to: http://www.erp.navy.mil/. To view Mr. Rosenthal's and Ms. Keen's biographies go to the Navy ERP Web site at http://www.erp.navy.mil and click on "Executive Bios." CHIPS

OMB Provides Updated Guidance for Reporting Incidents Involving Privacy Breaches

By the DON CIO Information Assurance Team

With recent reports of potential violations of sensitive personal information by federal agencies, the Office of Management and Budget (OMB) has tightened requirements for safeguarding information assets and for notification of security breaches.

Incidents Involving Personally Identifiable Information

The Federal Information Security Management Act (FISMA) requires all agencies to report security incidents involving personally identifiable information to the U.S. Computer Emergency Readiness Team (US-CERT), a federal incident response center located within the Department of Homeland Security. Personally identifiable information means any information about an individual maintained by an agency, including, but not limited to: education, financial transactions, medical history, and criminal or employment history, and information which can be used to distinguish or trace an individual's identity, such as name, Social Security Number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

Reporting Requirements

In a memo dated July 12, 2006, OMB provided updated guidance on the reporting of security incidents to now require agencies to report all incidents involving personally identifiable information to US-CERT within one hour of discovering the incident. The memo further stipulates that agencies should not distinguish between confirmed and suspected breaches, but to report all incidents, in both electronic and physical form. See the US-CERT Web site at http://www.us-cert.gov/federal/reportingRequirements.html for federal incident reporting guidelines. The Department of the Navy Chief Information Officer (DON CIO) is preparing to release additional guidance that will assist local commands with the specific processes for effectively handling privacy incidents.

Safeguarding Information

Earlier OMB guidance on agency compliance with FISMA called on all agencies to properly safeguard their information assets using a checklist developed by the National Institute for Standards and Technology (NIST). It calls for agencies to follow four steps: (1) Confirm identification of personally identifiable information protection needs; (2) Verify adequacy of organizational policy; (3) Implement protections for personally identifiable information being transported and/or stored off-site; and (4) Implement protections for remote access to personally identifiable information.

Taking these precautions should eliminate the need for reporting later.

The DON CIO is working to improve privacy protections for all DON information technology (IT) resources, collaborating with system owners throughout the Department to perform Privacy Impact Assessments (PIAs) on all relevant IT systems that handle personally identifiable information on DON military and civilian personnel. These PIAs, required by FISMA and DON CIO policy, provide a method for effectively measuring and analyzing the privacy protections in place throughout the Department. The DON CIO is also preparing to release revised policies regarding teleworking, remote access and data at rest that will include language outlining privacy protection requirements.

Contact DON CIO IA team member Darin Dropinski at darin.dropinski@navy.mil for more information. CHIPS